The Architecture of Perception: A Century of State Information Control and the Fracture of American Trust

By: Richard W. Vengels III

January 19, 2026

Introduction: The Control-Distrust Feedback Loop

The governance of information within the United States has undergone a fundamental transformation over the last century, evolving from a model of direct, analog intervention to a complex, privatized system of digital surveillance and cognitive management. This evolution is not merely a reaction to technological change but represents a concerted effort by the state apparatus to maintain narrative dominance in an increasingly fractured epistemological landscape. The historical trajectory, from the wiretaps of 1963 to the algorithmic "visibility filtering" of the 2020s, reveals a consistent institutional objective: the securing of public consensus as a critical component of national security.

However, the mechanisms employed to achieve this objective have shifted radically. Where the Cold War era relied on the "Institutional Trust" model, leveraging centralized gatekeepers in media and government to curate reality, the modern era faces the chaotic reality of "Distributed Trust," where authority is dispersed across peer-to-peer networks. In response, the U.S. intelligence and security communities have developed new doctrines, such as "Cognitive Warfare," which reclassify the domestic population's thoughts and beliefs as "cognitive infrastructure," a critical asset to be defended against "foreign malign influence" and domestic "malinformation."

This report provides an exhaustive analysis of this progression. It examines the documented history of U.S. intelligence media operations, the legal and doctrinal shifts that enabled the targeting of domestic audiences, and the rise of the "Censorship Industrial Complex", a network of public-private partnerships that circumvent First Amendment protections. Furthermore, it analyzes the sociological consequences of these actions, specifically the collapse of public trust and the deepening generational divide that threatens the social fabric of the nation. The analysis is grounded in declassified government documents, congressional testimony, academic research, and internal communications from social media platforms.

Part I: The Analog Era – Direct Intervention and the Origins of Media Management (1947–1976)

To understand the contemporary surveillance of the "cognitive domain," one must first examine the foundational structures of media influence established during the early Cold War. This era was characterized by direct, often covert, relationships between intelligence agencies and the press, justified by the existential threat of Soviet communism.

1.1 Project Mockingbird (1963): The Precedent of Executive Surveillance

While popular culture often conflates all CIA media activities under the umbrella of "Operation Mockingbird," the historical record reveals a distinct, highly specific operation authorized in 1963 known as **Project Mockingbird**. Unlike the broader recruitment of journalists, Project Mockingbird was a targeted surveillance operation designed to identify and plug leaks of classified information.[1]

Declassified documents from the CIA's Office of Security reveal that the project was initiated in March 1963 under the direct order of Director of Central Intelligence (DCI) John McCone, following discussions with President John F. Kennedy and Attorney General Robert F. Kennedy.[1] The impetus for the operation was the publication of articles by syndicated columnists **Robert S. Allen** and **Paul J. Scott**, whose "Allen-Scott Report" frequently contained highly accurate, classified intelligence regarding national security matters, including details on the Cuban Missile Crisis and advanced weapons systems.[1]

The operation involved the installation of wiretaps on the home telephones of both journalists and their shared office. The CIA's internal memos describe the operation as "extremely productive," revealing a vast network of sources that leaked information to the columnists. The surveillance logs captured conversations with high-ranking government officials, including:

- **Congressional Leadership:** Specific intercepts recorded conversations with Speaker of the House John McCormack.[1]
- **Executive Branch Officials:** Sources were identified within the White House, the Department of Defense, and the CIA itself.[1]
- **Other Journalists:** The taps revealed how Allen and Scott shared classified data with other reporters to obscure the original source.[1]

Crucially, the CIA noted that while some of the published information was "garbled," key points were "direct quotes from classified reports".[1] This concern over accurate but unauthorized information prefigures the modern government's focus on "malinformation", factually accurate information deemed harmful to national interests.

Project Mockingbird was terminated in June 1963, ostensibly to coincide with the retirement of the Director of Security, Sheffield Edwards, and due to the inherent political risks of wiretapping the press.[1] However, its existence establishes a critical historical fact: the surveillance of American journalists to control information flow was not a rogue activity but a sanctioned instrument of executive power, coordinated at the highest levels of the Kennedy administration.[2]

1.2 "Operation Mockingbird" and the "Mighty Wurlitzer"

Parallel to the specific surveillance of Project Mockingbird was a far more extensive program of media influence and asset recruitment, often retroactively termed "Operation Mockingbird." This structural effort was spearheaded by the Office of Policy Coordination (OPC) under Frank Wisner, who sought to create an apparatus capable of "playing any tune" the Agency desired, a concept he referred to as the "Mighty Wurlitzer".[9]

Investigation by journalist Carl Bernstein in 1977, along with subsequent historical analysis, documented that the CIA had maintained covert relationships with over 400 American journalists over a period of twenty-five years.[11] These relationships were not merely transactional; they were systemic. Assets were embedded in major news organizations, including *The New York Times*, *CBS*, *Time* magazine, and the *Washington Post*.[9]

The operational mechanics of this influence network relied on the centralization of media power:

- **Asset Placement:** The Agency recruited journalists to gather intelligence while on assignment abroad and to plant stories favorable to U.S. foreign policy.[9]
- **Editorial Cooperation:** Relationships with senior media executives allowed the CIA to suppress stories that threatened national security or to alter the framing of events to align with Cold War objectives.[9]
- **The "Blowback" Phenomenon:** While the statutory intent of these operations was to influence foreign audiences, stories planted in foreign outlets frequently "blew back" into the domestic U.S. press. This created a feedback loop where American citizens were inadvertently propagandized by their own government's disinformation campaigns abroad.[14]

This era epitomized the "Institutional Trust" model. The public's faith in the news was predicated on the perceived independence of media institutions. However, behind the veil of objectivity, a deep coordination existed between the security state and the Fourth Estate, managed through personal relationships among the elite class.

1.3 The Church Committee: Exposing the "Rogue Elephant"

The hermetic seal of this arrangement was broken in the 1970s. The Watergate scandal, combined with investigative reporting by Seymour Hersh regarding CIA domestic spying (Operation CHAOS), precipitated the formation of the **Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities**, commonly known as the **Church Committee**.[16]

Chaired by Senator Frank Church, the committee's 1975-1976 investigation provided the first comprehensive public audit of the U.S. intelligence community. The findings were staggering, revealing a pattern of abuse that extended far beyond media manipulation:

- **Operation SHAMROCK:** The committee exposed that the National Security Agency (NSA) had systematically intercepted millions of telegrams entering and leaving the United States for decades, utilizing the cooperation of major telecommunications companies, a direct precursor to modern bulk data collection.[19]

- **Operation MKULTRA:** The investigation uncovered CIA programs involving human experimentation with LSD and other psychoactive drugs to develop mind control techniques.[19]
- **COINTELPRO:** The FBI was found to have engaged in extensive covert action to disrupt, discredit, and neutralize domestic political organizations, including civil rights groups and anti-war activists.[18]

Senator Church's warning regarding the NSA's capabilities remains one of the most prescient statements in the history of surveillance:

> "I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return." [19]

The Church Committee led to significant reforms, including the establishment of the Senate Select Committee on Intelligence (SSCI) and the passage of the Foreign Intelligence Surveillance Act (FISA) of 1978.[17] However, critics argue that these reforms did not end the intelligence community's influence over the media but merely formalized and regulated it. In 1996, CIA Director John Deutch admitted to Congress that the Agency retained the authority to use journalists and clergy as assets in "exceptional circumstances," preserving a loophole that would become relevant in the digital age.[12]

Part II: The Legal and Doctrinal Transition (1980–2016)

Following the reforms of the 1970s, the mechanisms of information control evolved. The focus shifted from direct asset recruitment to legal and doctrinal redefinitions that would allow for the integration of information operations into a broader spectrum of conflict.

2.1 The Smith-Mundt Modernization Act (2012): Dissolving the Firewall

A pivotal moment in the legal framework of U.S. information operations occurred with the passage of the **Smith-Mundt Modernization Act of 2012**, incorporated into the National Defense Authorization Act (NDAA) for Fiscal Year 2013.[22]

The original **Smith-Mundt Act of 1948** (United States Information and Educational Exchange Act) authorized the State Department to engage in public diplomacy abroad (e.g., Voice of America, Radio Free Europe) but explicitly prohibited the domestic dissemination of these materials. This prohibition was intended as a firewall to prevent the U.S. government from propagandizing its own citizens.[15]

The 2012 modernization effectively repealed this ban. Proponents of the legislation, including Rep. Mac Thornberry and Rep. Adam Smith, argued that the restriction was obsolete in the internet age, where geographic boundaries for information were meaningless. They contended that the reform would promote transparency by allowing Americans to see what their government was broadcasting overseas.[25]

However, critics and civil libertarians viewed this as a dangerous expansion of state power. By removing the domestic dissemination ban, the government was legally authorized to direct information operations, crafted for foreign psychological warfare, at the American public.[27] The legislation blurred the line between "public diplomacy" (foreign) and "public affairs" (domestic), creating a legal environment where government-produced narratives could circulate freely within the domestic news cycle without the previous statutory hindrances.[29]

2.2 The Evolution of Military Doctrine: Information Operations (IO)

Concurrent with legal changes, U.S. military doctrine was undergoing a conceptual shift regarding the nature of information in warfare. Throughout the 1990s and 2000s, the Department of Defense (DoD) refined its approach to **Information Operations (IO)**.

Joint Publication 3-13 (Information Operations) defined IO as the integrated employment of electronic warfare, computer network operations, psychological operations (PSYOP), military deception, and operations security to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own.[31]

Initially, IO was strictly strictly delineated as a tool for foreign adversaries. However, the concept of the **"Gray Zone"**, conflict falling below the threshold of conventional war, began to erode these boundaries. Military strategists increasingly viewed the "Information Environment" (IE) as a unitary battlespace. The rise of the internet meant that an information operation conducted against a foreign target (e.g., a jihadist forum) inevitably had domestic bleed-over. The doctrine began to emphasize "narrative control" and "perception management" as essential components of strategic victory, setting the stage for the domestic application of these techniques under the guise of "defense".[32]

Part III: The Digital Panopticon – The "Censorship Industrial Complex" (2016–2023)

The shock of the 2016 presidential election served as a catalyst for the rapid expansion of domestic information control infrastructure. Framing the election outcome as the result of foreign "disinformation," the federal government, in coordination with private tech companies and academic institutions, constructed a vast apparatus to monitor and curate domestic speech. This network has been described by congressional investigators and civil liberties advocates as the "Censorship Industrial Complex."

3.1 CISA and the Redefinition of "Infrastructure"

The cornerstone of this modern apparatus is the **Cybersecurity and Infrastructure Security Agency (CISA)**, established within the Department of Homeland Security (DHS) in 2018.[34] While its statutory mission was to protect physical critical infrastructure (e.g., dams, power grids) and cybersecurity, CISA quickly expanded its remit to include the "information ecosystem."

This mission creep was explicitly articulated by CISA Director Jen Easterly in 2021:

> **"One could argue we're in the business of critical infrastructure, and the most critical infrastructure is our cognitive infrastructure, so building that resilience to misinformation and disinformation, I think, is incredibly important."** [34]

By designating the American mind, "cognitive infrastructure", as a critical asset, CISA asserted jurisdiction over what Americans think and believe. To operationalize this, CISA formed the **MDM (Mis-, Dis-, and Malinformation) team**. The definitions adopted by CISA are critical to understanding the scope of this control:

- **Misinformation:** Information that is false, but not created or shared with the intention of causing harm.
- **Disinformation:** Information that is false and deliberately created to mislead, harm, or manipulate.
- **Malinformation: "Information that is based on fact, but used out of context to mislead, harm, or manipulate."**.[37]

The category of **malinformation** represents a profound departure from traditional First Amendment norms. It allows the security state to target *factually true* information if it contradicts official narratives or is deemed to undermine public trust. This effectively deputizes the government as the arbiter of context and intent, not just factual veracity.

3.2 The Election Integrity Partnership (EIP): Censorship by Proxy

Recognizing that the First Amendment prohibits the government from directly censoring protected speech, federal agencies engaged in "censorship by proxy" through public-private partnerships. The most prominent of these was the **Election Integrity Partnership (EIP)**, formed in 2020.[41]

The EIP was a consortium comprising the **Stanford Internet Observatory (SIO)**, the University of Washington's Center for an Informed Public, Graphika, and the Atlantic Council's Digital Forensic Research Lab.[42] The partnership worked in direct coordination with CISA, the State Department's **Global Engagement Center (GEC)**, and the **Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)** to monitor and flag election-related speech.[41]

The Mechanism of Control: Jira Tickets

The operational heart of the EIP was a Jira ticketing system, a project management software used to track and triage censorship requests. The workflow, as revealed by internal documents and congressional reports, functioned as follows:

1. **Stakeholder Reporting:** "External stakeholders", including federal agencies (CISA, DHS), state officials, and trusted partners, submitted reports of "misinformation" directly to the EIP.[42]
2. **Analyst Review:** EIP analysts assessed the reports and scoured social media platforms for similar content, often using keyword searches to identify emerging narratives.
3. **Platform Switchboarding:** The EIP compiled lists of URLs and accounts and transmitted them to Big Tech companies (Twitter, Facebook, Google, TikTok, Reddit) via the Jira system. These "tickets" contained specific recommendations for enforcement, ranging from content removal and labeling to **"visibility filtering"** (shadow banning) and account suspension.[42]

In the lead-up to the 2020 election, the EIP processed hundreds of tickets targeting millions of posts. The targets were disproportionately domestic political speech, including posts by elected officials, media outlets, and ordinary citizens. By routing these requests through the EIP, the government could claim it was not directly ordering censorship, while the platforms could claim they were merely acting on the advice of "independent experts".[41]

3.3 The Virality Project: Policing Health Narratives

Following the 2020 election, the infrastructure of the EIP was repurposed to address COVID-19 vaccine discourse under the name **The Virality Project** (2021).[44] The scope of this project expanded beyond false claims to explicitly target "narratives" that questioned public health policies.

Internal documents and weekly briefings from the Virality Project reveal a systematic effort to suppress **"true content"** that might "fuel hesitancy." The project's analysts flagged:

- **True Stories of Side Effects:** Personal testimonies and news reports regarding genuine vaccine side effects were categorized as "malinformation" because they could discourage vaccination.[48]
- **Scientific Debate:** Discussion of natural immunity, the lab leak theory, and the efficacy of mandates, topics that were subjects of legitimate scientific debate, were targeted for suppression.[49]
- **Global Policy Context:** Reports on other countries (e.g., European nations restricting certain vaccines for specific age groups) were flagged as "misleading" in the U.S. context.[49]

The "Twitter Files" and "Facebook Files" confirmed that platforms frequently acceded to this pressure, modifying their moderation policies to accommodate government demands. Facebook executives, for instance, acknowledged in internal emails that they were removing content that was "often-true" under pressure from the Biden White House.[49]

3.4 The "Hamilton 68" Deception and False Flags

A critical component of the information control architecture is the manufacturing of the "foreign influence" threat to justify domestic censorship. A prime example of this is the **Hamilton 68** dashboard, launched in 2017 by the Alliance for Securing Democracy (ASD), a project of the German Marshall Fund.[52]

Hamilton 68 purported to track "Russian bots" and influence operations on Twitter in real-time. Its data was cited extensively by major media outlets (*The New York Times*, *Washington Post*, *MSNBC*, *Mother Jones*) and members of Congress to attribute organic political hashtags (such as #ReleaseTheMemo) to Russian interference.[54]

However, the release of the Twitter Files in 2022 exposed Hamilton 68 as a methodological fraud. Internal emails from Twitter's Trust and Safety team, including Yoel Roth, revealed that the company had reverse-engineered the Hamilton 68 list and found that the accounts were not Russian spies or bots. Roth wrote:

> **"Hamilton 68 barely had any Russians... Instead of tracking how 'Russia' influenced American attitudes, Hamilton 68 simply collected a handful of mostly real, mostly American accounts and described their organic conversations as Russian scheming."**.[53]

The list consisted largely of ordinary American citizens with right-leaning views. By falsely labeling these citizens as Russian assets, Hamilton 68 and the media outlets that amplified it engaged in a disinformation campaign of their own, generating public hysteria that facilitated stricter censorship policies.[58]

3.5 The Global Engagement Center (GEC) and Ad-Revenue Blacklisting

The **Global Engagement Center (GEC)**, located within the State Department, is statutorily mandated to counter foreign propaganda. However, investigations have revealed that GEC funded entities that targeted the domestic American press. Specifically, GEC provided grants to the **Global Disinformation Index (GDI)**, a British organization that rates news outlets based on their "disinformation risk".[60]

GDI produces **"dynamic exclusion lists"**, blacklists of websites deemed high-risk, which are fed to advertising technology companies (such as Microsoft's Xandr). This effectively demonetizes the listed outlets by blocking ads from appearing on their sites.

GDI's methodology displayed systemic ideological bias. Its reports consistently labeled conservative and libertarian outlets (e.g., *Reason*, *New York Post*, *The Federalist*, *RealClearPolitics*) as "high risk," while rating liberal outlets (e.g., *NPR*, *The New York Times*, *HuffPost*) as "low risk" or "neutral".[63] By funding GDI, the State Department effectively subsidized a mechanism to financially cripple domestic media organizations that criticized administration policies, a violation of the spirit, if not the letter, of the non-intervention principle. This controversy was a key factor in Congress declining to renew GEC's legislative authority in late 2024.[60]

Part IV: The Doctrine of Cognitive Warfare – The Mind as Battlespace

The operational shift toward domestic information control is underpinned by a profound evolution in military doctrine: the emergence of **Cognitive Warfare**. This concept transcends "Information Operations" to view the human mind itself as the decisive terrain of conflict.

4.1 Defining the Cognitive Domain

Military strategists and NATO researchers have formally identified the **"Human Domain"** or **"Cognitive Domain"** as the sixth domain of warfare, alongside land, sea, air, space, and cyber.[67]

A 2020 NATO-sponsored study defines Cognitive Warfare as:

> **"The art of using technologies to alter the cognition of human targets... it involves hacking the individual to alter the way they think, how they perceive, and how they act."** [68]

Unlike psychological operations (PSYOP), which aim to influence specific attitudes, Cognitive Warfare seeks to disrupt the cognitive mechanisms of a population, their ability to process information, distinguish truth from falsehood, and maintain resilience. The goal is "Cognitive Superiority," defined as the ability to seize the initiative in the cognitive domain.[70]

4.2 Targeting the OODA Loop

Doctrinally, Cognitive Warfare targets the **OODA Loop** (Observe, Orient, Decide, Act) of a target population [70]:

1. **Observe:** Control the inputs (censorship, algorithmic curation, "visibility filtering").
2. **Orient:** Shape the interpretation of data (fact-checking labels, narrative framing, "malinformation" designations).
3. **Decide:** Influence the cognitive processing to ensure alignment with strategic goals.
4. **Act:** Engineer specific behavioral outcomes (voting patterns, compliance with mandates, social mobilization).

By framing domestic "cognitive infrastructure" as a national security asset, the government asserts the authority to secure the OODA loops of its own citizens. This justifies the monitoring of social media not merely as intelligence gathering, but as active "defense" of the national mind against "cognitive attacks" (dissenting narratives).[71]

4.3 Malinformation as a Cognitive Threat

In this framework, **malinformation**, truth used to cause harm, is viewed as a potent cognitive weapon. If the strategic objective is to maintain a unified public perception (Cognitive Security), then factual information that disrupts that unity is interpreted as an attack on the system's resilience.[69] This doctrinal logic explains why the Virality Project targeted true stories of vaccine side effects; the veracity of the information was secondary to its potential to disrupt the "cognitive resilience" of the population regarding the vaccination campaign.

Part V: Sociological Consequences – The Collapse of Trust and Generational Division

The intensification of state information control is inextricably linked to a profound sociological shift in how trust is constructed and maintained. As the government attempts to reassert control via "Institutional Trust" mechanisms, society is migrating toward "Distributed Trust," creating a dangerous friction.

5.1 Botsman's Trust Transition: From Institutional to Distributed

Sociologist Rachel Botsman identifies three distinct eras of trust in human history:

1. **Local Trust:** Interpersonal, community-based, limited by geography.
2. **Institutional Trust:** Placed in centralized hierarchies (governments, banks, media corporations). This model defined the 20th century.
3. **Distributed Trust:** Placed in networks, peers, and decentralized platforms (blockchain, social media, encrypted chat). This defines the digital age.[75]

Table 1: The Trust Paradigm Shift

Feature	**Institutional Trust (20th Century)**	**Distributed Trust (21st Century)**
Source of Authority	Hierarchical, Top-Down, Expert-led	Networked, Peer-to-Peer, Crowdsourced
Verification	Credentials, Brand Reputation	Transparency, User Reviews, Blockchain

Information Flow	Broadcast (One-to-Many)	Networked (Many-to-Many)
Gatekeepers	Editors, Regulators, Officials	Algorithms, Community Notes, Influencers
Response to Failure	Reform, Regulatory Oversight	Exit, Forking, Cancellation

5.2 The Collapse of Institutional Trust

We are currently witnessing the catastrophic collapse of **Institutional Trust**. Data from Pew Research indicates that public trust in the federal government has plummeted from a high of roughly 77% in 1964 (the Johnson administration) to near-historic lows of approximately 17-20% in the 2020s.[78]

This decline is not merely a result of "disinformation" but a consequence of repeated institutional failures and the opacity of the centralized model (e.g., Vietnam, Watergate, WMDs in Iraq, the 2008 Financial Crisis). The government's response, adopting the tactics of Project Mockingbird and the CISA "Cognitive Infrastructure" model, is an attempt to *force* Institutional Trust by eliminating alternatives. By censoring "misinformation" and controlling narratives, institutions attempt to re-establish their monopoly on truth.

5.3 The Generational Divide and Epistemic Crisis

This dynamic creates a sharp generational and epistemological fracture:

- **Older Generations (Boomers/Gen X):** Raised in the era of Institutional Trust, these cohorts retain a higher baseline faith in legacy media and government spokespeople. They are more likely to view "fact-checks" and intelligence assessments as authoritative and protective.[81]
- **Younger Generations (Millennials/Gen Z):** Natives of **Distributed Trust**. They inherently distrust centralized gatekeepers. They seek verification through peer networks, community notes, and decentralized sources. To this demographic, "content moderation" by a central authority is perceived not as protection, but as manipulation and gaslighting.[83]

The result is an **Epistemic Crisis**, a fragmentation of shared reality.[85] The government's attempt to impose a single "authoritative" narrative via censorship directly clashes with the distributed nature of the internet.

- **The Backfire Effect:** When institutions are caught censoring true information (malinformation) or pushing falsehoods (Hamilton 68), the breach of trust is catastrophic. It validates the "conspiracy theories" of the distributed networks, pushing the population further toward radical decentralization and skepticism.[87]

- **Polarization:** This drives the population into separate information ecosystems. One ecosystem is curated by the state/corporate "trust and safety" apparatus; the other is a chaotic landscape of distributed, often unverified, counter-narratives. The common ground necessary for democratic debate evaporates.[89]

Conclusion: The Fracture of the American Mind

The documented history of U.S. information control reveals a consistent, century-long objective: the maintenance of narrative dominance by the state. From the crude wiretaps of **Project Mockingbird** in 1963 to the sophisticated **Jira tickets** of the **Election Integrity Partnership** in 2020, the goal remains the same: to identify and neutralize information that threatens institutional consensus.

However, the modern execution of this goal through **public-private partnerships** and the doctrine of **Cognitive Warfare** has fundamentally altered the relationship between the government and the governed. By redefining the American mind as "critical infrastructure" to be secured, the state has engaged in a form of preemptive warfare against its own citizens' cognition. The definition of **malinformation**, the censorship of truth to protect narrative, signals that the priority of the security state is no longer factual accuracy but **cognitive compliance**.

This strategy is proving historically counterproductive. The sociological shift toward **Distributed Trust** means that attempts to reimpose centralized control are met with increasing resistance. The exposure of operations like **Hamilton 68** and the **Virality Project** confirms to the public that their institutions are acting as combatants in an information war rather than neutral arbiters of truth.

The long-term consequence is a society where trust is not recovered but shattered further. The "Cognitive Infrastructure" is not being secured; it is being Balkanized. As the government tightens its grip on the narrative to manufacture consensus, it inadvertently accelerates the fragmentation and radicalization it claims to be fighting. The wiretaps on two reporters in 1963 have metastasized into a surveillance grid encompassing the entire digital public square, leaving the American social fabric more divided, paranoid, and fragile than at any point in modern history.

Summary of Key Entities and Mechanisms of Control

Entity	Role in Information Control	Key Mechanism

CISA (DHS)	"Quarterback" of domestic censorship; defines "Cognitive Infrastructure."	**MDM** definitions; designating thought as infrastructure; Rumor Control.
GEC (State Dept)	Counter-propaganda arm; funded domestic blacklisting tools.	Funding **GDI** & **NewsGuard**; blurring foreign/domestic operations.
EIP / Virality Project	NGO consortium acting as government proxy for censorship.	**Jira Tickets**; "Switchboarding" flags to Big Tech; targeting "true content."
Hamilton 68	Dashboard used to falsely attribute domestic speech to Russia.	**False Flag** data analytics; media amplification loop; labeling Americans as "bots."
Project Mockingbird	CIA surveillance of journalists (1963).	**Wiretaps** to identify leaks; historical precedent for executive surveillance.
Cognitive Warfare	Military doctrine treating the mind as a battlespace.	**OODA Loop** disruption; targeting resilience/will; "Human Domain" operations.

Works cited

1. PROJECT MOCKINGBIRD[15770719].pdf
2. Project Mockingbird - Wikipedia, accessed January 18, 2026, https://en.wikipedia.org/wiki/Project_Mockingbird
3. Project Mockingbird: From 1963 Wiretaps To Enduring Digital ..., accessed January 18, 2026, https://www.odrindia.in/2025/10/10/project-mockingbird-from-1963-wiretaps-to-enduring-digital-surveillance-echoes/
4. PROJECT MOCKINGBIRD[15770719].pdf - CIA, accessed January 18, 2026,

https://www.cia.gov/readingroom/docs/PROJECT%20MOCKINGBIRD%5B15770719%5D.pdf
5. CIA director personally intervenes in press wiretapping matter, accessed January 18, 2026, https://www.rcfp.org/cia-paul-scott-project-mockingbird/
6. PROJECT MOCKINGBIRD TRANSCRIPTS AND ADDITIONAL ..., accessed January 18, 2026, https://www.cia.gov/readingroom/document/06555844
7. O-R (IV-FF), Project MOCKINGBIRD, accessed January 18, 2026, https://www.fordlibrarymuseum.gov/library/document/0180/75573204.pdf
8. Project Mockingbird - Truth Revolution Of 2025 By Praveen Dalal, accessed January 18, 2026, https://odrindia.in/wiki/Project_Mockingbird
9. The CIA and journalism - SourceWatch, accessed January 18, 2026, https://www.sourcewatch.org/index.php/The_CIA_and_journalism
10. Mockingbird Media Framework - ODR India, accessed January 18, 2026, https://odrindia.in/wiki/Mockingbird_Media_Framework
11. Operation Mockingbird - Wikipedia, accessed January 18, 2026, https://en.wikipedia.org/wiki/Operation_Mockingbird
12. The CIA's Secret Ties To Reporters And Church Leaders: A Plain Story, accessed January 18, 2026, https://www.odrindia.in/2025/10/10/the-cias-secret-ties-to-reporters-and-church-leaders-a-plain-story/
13. Operation Mockingbird - Spartacus Educational, accessed January 18, 2026, https://spartacus-educational.com/JFKmockingbird.htm
14. Operation Mockingbird: From Cold War Covert Ops to 2025 ... - FYIVT, accessed January 18, 2026, https://fyivt.com/be-informed/operation-mockingbird-from-cold-war-covert-ops-to-2025-whistleblowers/
15. Propaganda? So what? - American Security Project, accessed January 18, 2026, https://www.americansecurityproject.org/propaganda-so-what/
16. CIA Assassination Plots: The Church Committee Report 50 Years ..., accessed January 18, 2026, https://nsarchive.gwu.edu/briefing-book/intelligence/2025-11-20/cia-assassination-plots-church-committee-report-50-years
17. Senate Select Committee to Study Governmental Operations with ..., accessed January 18, 2026, https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm
18. A History of Notable Senate Investigations: The Church Committee, accessed January 18, 2026, https://www.senate.gov/about/resources/pdf/church-committee-full-citations.pdf
19. Church Committee - Wikipedia, accessed January 18, 2026, https://en.wikipedia.org/wiki/Church_Committee
20. Looking back at the Church Committee | Constitution Center, accessed January 18, 2026, https://constitutioncenter.org/blog/looking-back-at-the-church-committee
21. Why Church Committee alums urged new House panel to avoid ..., accessed January 18, 2026, https://hls.harvard.edu/today/why-church-committee-alums-urged-new-house-panel-to-avoid-partisanship/
22. (PDF) The Effects of Smith-Mundt Act on U.S. Public Diplomacy in ..., accessed January 18, 2026, https://www.researchgate.net/publication/379564736_The_Effects_of_Smith-Mundt_Act_on_US_Public_Diplomacy_in_the_Digital_Age
23. 112th Congress (2011-2012): Smith-Mundt Modernization Act of 2012, accessed January 18, 2026, https://www.congress.gov/bill/112th-congress/house-bill/5736

24. Smith–Mundt Act - Wikipedia, accessed January 18, 2026, https://en.wikipedia.org/wiki/Smith%E2%80%93Mundt_Act
25. Smith-Mundt Belatedly Enters the 21st Century, accessed January 18, 2026, https://uscpublicdiplomacy.org/pdin_monitor_article/smith-mundt-belatedly-enters-21st-century
26. New Government “Propaganda” Bill a Positive Step for First ... - ACLU, accessed January 18, 2026, https://www.aclu.org/news/free-speech/new-government-propaganda-bill-positive-step-first-amendment
27. Apple Pie Propaganda? The Smith–Mundt Act Before and After the ..., accessed January 18, 2026, https://northwesternlawreview.org/issues/apple-pie-propaganda-the-smith-mundt-act-before-and-after-the-repeal-of-the-domestic-dissemination-ban/
28. U.S. Public Diplomacy: Legislative Proposals to Amend Prohibitions ..., accessed January 18, 2026, https://www.everycrsreport.com/reports/R42754.html
29. The Blogosphere Worries about Government Propaganda, accessed January 18, 2026, https://www.pewresearch.org/journalism/2012/05/31/blogosphere-worries-about-government-propaganda/
30. apple pie propaganda? the smith–mundt act before and after the ..., accessed January 18, 2026, https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1203&context=nulr
31. Defense Primer: Operations in the Information Environment, accessed January 18, 2026, https://www.congress.gov/crs-product/IF10771
32. Information Operations as a Deterrent to Armed Conflict, accessed January 18, 2026, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20100630_art014.pdf
33. Military Information Support Operations, accessed January 18, 2026, https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/Military_Information_Support_Operations.pdf
34. The Weaponization of CISA: How a 'Cybersecurity' Agency Colluded ..., accessed January 18, 2026, https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf
35. Grassley to CISA - Critical Infrastructure, accessed January 18, 2026, https://www.grassley.senate.gov/download/grassley-to-cisa_-critical-infrastructure
36. "Censorship Laundering: How the U.S. Department of Homeland ..., accessed January 18, 2026, https://www.congress.gov/event/118th-congress/house-event/115901/text
37. Preparing for and Mitigating Foreign Influence Operations Targeting ..., accessed January 18, 2026, https://www.cisa.gov/sites/default/files/2023-01/cisa_insight_mitigating_foreign_influence_508.pdf
38. Myths and Misconceptions - Marion County, accessed January 18, 2026, https://www.co.marion.or.us/CO/elections/Pages/Myths.aspx
39. Disinformation Stops With You Infographic Set - CISA, accessed January 18, 2026, https://www.cisa.gov/sites/default/files/publications/disinformation_stops_with_you_infographic_set_508.pdf
40. Elections & Misinformation | Office of Homeland Security, accessed January 18, 2026, https://law.hawaii.gov/ohs/elections/
41. written testimony - Congress.gov, accessed January 18, 2026,

https://www.congress.gov/118/meeting/house/115611/witnesses/HHRG-118-FD00-Wstate-LandryJ-20230330.pdf

42. the weaponization of “disinformation” pseudo-experts and, accessed January 18, 2026, https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/EIP_Jira-Ticket-Staff-Report-11-7-23-Clean.pdf
43. The Censorship Industrial Complex: What Are Trump And Musk ..., accessed January 18, 2026, https://swarajyamag.com/ideas/the-censorship-industrial-complex-what-are-trump-and-musk-trying-fo-fight
44. Background on the SIO's Projects on Social Media - Congress.gov, accessed January 18, 2026, https://www.congress.gov/118/meeting/house/115561/documents/HHRG-118-IF16-20230328-SD078.pdf
45. Stanford Internet Observatory - Wikipedia, accessed January 18, 2026, https://en.wikipedia.org/wiki/Stanford_Internet_Observatory
46. How the Federal Government Partnered with Universities, accessed January 18, 2026, https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/eip-jira-report-key-takeaways-one-pager-11.6.23.pdf
47. Censorship Industrial Complex, Part 2, accessed January 18, 2026, https://docs.house.gov/meetings/FD/FD00/20231130/116615/HHRG-118-FD00-Wstate-ShellenbergerM-20231130.pdf
48. COVID Censorship: Yes, Biden Admin. Suppressed Free Speech ..., accessed January 18, 2026, https://www.acsh.org/news/2024/02/25/covid-censorship-yes-biden-admin-suppressed-free-speech-during-pandemic-17678
49. the censorship-industrial complex: how top biden white house, accessed January 18, 2026, https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/Biden-WH-Censorship-Report-final.pdf
50. Newly released emails show coordination between social media ..., accessed January 18, 2026, https://docs.house.gov/meetings/GO/GO02/20220914/115106/HHRG-117-GO02-20220914-SD012.pdf
51. Zuckerberg says the White House pressured Facebook to 'censor ..., accessed January 18, 2026, https://www.pbs.org/newshour/politics/zuckerberg-says-the-white-house-pressured-facebook-to-censor-some-covid-19-content-during-the-pandemic
52. How to Interpret the Hamilton 68 Dashboard — Key Points and ..., accessed January 18, 2026, https://www.gmfus.org/how-interpret-hamilton-68-dashboard-key-points-and-clarifications
53. A Guide to Understanding the Hoax of the Century, accessed January 18, 2026, https://www.hsgac.senate.gov/wp-content/uploads/Testimony-Siegel-2023-05-16-2.pdf
54. Twitter Files Journalists - Supreme Court of the United States, accessed January 18, 2026, https://www.supremecourt.gov/DocketPDF/23/23-411/300197/20240208220913623_44722%20pdf%20Candeub.pdf
55. Censorship Industrial Complex - Document Repository, accessed January 18, 2026, https://docs.house.gov/meetings/IF/IF16/20230328/115561/HHRG-118-IF16-20230328-SD012.pdf
56. TRUTH Always Wins - Penn State Research Database, accessed January 18, 2026, https://pure.psu.edu/ws/portalfiles/portal/75862603/HartmanCaverly_LibsPromReflDial_Ch9TruthAlwaysWins.pdf
57. Washington Post forced to issue several corrections on 'Russian bot ..., accessed January

18, 2026, https://www.foxnews.com/media/washington-post-forced-issue-several-corrections-russian-bot-stories-following-twitter-files

58. Alliance for Securing Democracy - InfluenceWatch, accessed January 18, 2026, https://www.influencewatch.org/non-profit/alliance-for-securing-democracy/
59. Lessons from Year One of Hamilton 68, accessed January 18, 2026, https://securingdemocracy.gmfus.org/a-view-from-the-digital-trenches-lessons-from-year-one-of-hamilton-68/
60. Censorship-Industrial Complex - House.gov, accessed January 18, 2026, https://docs.house.gov/meetings/FA/FA19/20250401/118072/HHRG-119-FA19-Wstate-WeingartenB-20250401.pdf
61. McCaul, Mast, Issa Send Letter Expressing Concerns with GEC ..., accessed January 18, 2026, https://foreignaffairs.house.gov/news/press-releases/mccaul-mast-issa-send-letter-expressing-concerns-with-gec-reauthorization
62. Policy Brief: Dismantle Entities Actively Censoring Americans, accessed January 18, 2026, https://americarenewing.com/policy-brief-dismantle-entities-actively-censoring-americans/
63. The U.S. State Department Funds an Ad-Blacklisting Group. It ..., accessed January 18, 2026, https://www.cato.org/blog/us-state-department-funds-ad-blacklisting-group-it-shouldnt
64. Global Disinformation Index's Risk Assessment Shows Bias Against ..., accessed January 18, 2026, https://www.allsides.com/blog/misinformation-watch-disinformation-risk-assessment-lacks-transparency-shows-bias-against-right
65. Global Disinformation Index (GDI) - InfluenceWatch, accessed January 18, 2026, https://www.influencewatch.org/organization/global-disinformation-index-gdi/
66. State Department's disinformation office to close after funding nixed ..., accessed January 18, 2026, https://cyberscoop.com/state-departments-disinformation-office-to-close-after-funding-nixed-in-ndaa/
67. Cognitive Warfare The Fight for Gray Matter in the Digital Gray Zone, accessed January 18, 2026, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3853187/cognitive-warfare-the-fight-for-gray-matter-in-the-digital-gray-zone/
68. Cognitive Warfare | PDF | Politics - Scribd, accessed January 18, 2026, https://www.scribd.com/document/695151061/Cognitive-Warfare
69. Cognitive Warfare to Dominate and Redefine Adversary Realities, accessed January 18, 2026, https://sofsupport.org/cognitive-warfare-to-dominate-and-redefine-adversary-realities-implications-for-u-s-special-operations-forces/
70. Cognitive Warfare: An Allied Blueprint and a Pentagon Opportunity, accessed January 18, 2026, https://smallwarsjournal.com/2026/01/16/cognitive-warfare/
71. National Cognitive Infrastructure Protection: What Can We Learn ..., accessed January 18, 2026, https://oodaloop.com/analysis/decision-intelligence/national-cognitive-infrastructure-protection-what-can-we-learn-from-the-swedish-psychological-defence-authority/
72. Mitigating Risks To America's Cognitive Infrastructure - OODAloop, accessed January 18, 2026, https://oodaloop.com/analysis/decision-intelligence/mitigating-risks-to-americas-cognitive-infrastructure/
73. Securing Election Infrastructure Against the Tactics of Foreign ..., accessed January 18,

2026, https://www.hsdl.org/c/view?docid=887542

74. Smoke and mirrors: Building EU resilience against manipulation ..., accessed January 18, 2026, https://www.iss.europa.eu/publications/briefs/smoke-and-mirrors-building-eu-resilience-against-manipulation-through-cognitive
75. Local Marketing Insider #019 // What is Distributed Trust? - Widewail, accessed January 18, 2026, https://www.widewail.com/blog/local-marketing-insider-019
76. Ian Bremmer, Rachel Botsman and Azeem Azhar: 3 experts on the ..., accessed January 18, 2026, https://www.weforum.org/podcasts/radio-davos/episodes/risk-trust-geopolitics-2024-bremmer-botsman-azhar/
77. Build stronger trust on your teams, with Rachel Botsman, accessed January 18, 2026, https://mastersofscale.com/build-stronger-trust-on-your-teams/
78. Let's play a drinking game - Government Executive, accessed January 18, 2026, https://www.govexec.com/management/2026/01/lets-play-drinking-game/410729/
79. Public Trust in Government: 1958-2025 - Pew Research Center, accessed January 18, 2026, https://www.pewresearch.org/politics/2025/12/04/public-trust-in-government-1958-2025/
80. Americans' Deepening Mistrust of Institutions, accessed January 18, 2026, https://www.pew.org/en/trend/archive/fall-2024/americans-deepening-mistrust-of-institutions
81. Are Americans Losing Their Trust? - Skeptic Research Center, accessed January 18, 2026, https://research.skeptic.com/content/files/2025/02/Research-Report-PADS-010.pdf
82. Trust in government by generation - Pew Research Center, accessed January 18, 2026, https://www.pewresearch.org/chart/trust-in-government-by-generation/
83. & news media inAustralia - UTS, accessed January 18, 2026, https://www.uts.edu.au/globalassets/sites/default/files/2018-09/pdf_4_flipbook.pdf
84. The Construction of Distributed Trust on Bilibili Under the COVID-19 ..., accessed January 18, 2026, https://www.researchgate.net/publication/381302698_The_Construction_of_Distributed_Trust_on_Bilibili_Under_the_COVID-19_Pandemic
85. Media, Knowledge and Trust: The Deepening Epistemic Crisis of ..., accessed January 18, 2026, https://www.semanticscholar.org/paper/Media%2C-Knowledge-and-Trust%3A-The-Deepening-Epistemic-Dahlgren/7ed7b615061369f877e61ae67a54b61b4b1d574c
86. Epistemological crises in violent contexts during the age of (dis ..., accessed January 18, 2026, https://www.crg-ghent.be/wp-content/uploads/2023/06/01_Epistemological-crises-in-violent-contexts-during-the-age-of-disinformation.pdf
87. Who Can You Trust? How Technology Brought Us Together and ..., accessed January 18, 2026, https://www.scribd.com/document/971418778/Who-Can-You-Trust-How-Technology-Brought-Us-Together-and-Why-It-Might-Drive-Us-Apart-ISBN-9781541773677-1541773675-High-Quality-eBook
88. Who Can You Trust? PDF - Bookey, accessed January 18, 2026, https://cdn.bookey.app/files/pdf/book/en/who-can-you-trust-.pdf
89. Media Mistrust Has Been Growing for Decades—Does It Matter?, accessed January 18, 2026, https://www.pew.org/en/trend/archive/fall-2024/media-mistrust-has-been-growing-for-decades-does-it-matter